UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. RUSLANS BONDARS, a/k/a, "Ruslan Bondar," and JURIJS MARTIŠEVS, a/k/a, "Yury Martyshev," "Jurijs Bereverovs" Defendants	Criminal No. 1:16-cr-228 Count 1: 18 U.S.C. § 371 Conspiracy Count 2: 18 U.S.C. § 1349 Conspiracy to Commit Wire Fraud Count 3: 18 U.S.C. §§ 1343 & 2 Wire Fraud & Aiding and Abetting Count 4: 18 U.S.C. §§ 2 & 1030(a)(5)(A) Computer Intrusion With Intent to Damage & Aiding and Abetting Notice of Forfeiture **UNDER SEAL**

INDICTMENT

October 2016 Term — at Alexandria, Virginia

Introduction

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

1. Defendant RUSLANS BONDARS was a permanent resident of Latvia who resided in Riga, Latvia. BONDARS sometimes went by the first name Ruslan and the last name Bondar.

2. Defendant JURIJS MARTIŠEVS was a citizen of Latvia who resided in Riga, Latvia and Moscow, Russia. MARTIŠEVS sometimes went by the last names "Martyshev" and "Bereverovs." MARTIŠEVS sometimes went by the first name "Yury."

3. Amazon Web Services operated servers in the Eastern District of Virginia upon which it offered cloud storage services.

4. ICQ was an instant messaging service that employed servers located within the Eastern District of Virginia.

5. The above introductory allegations are realleged and incorporated in each count of this Indictment as though fully set out in each count.

COUNT 1

18 U.S.C. § 371
(Conspiracy)

THE GRAND JURY FURTHER CHARGES THAT:

6. From at least on or about October 3, 2006, and continuing until at least the date of this Indictment, in the Eastern District of Virginia and elsewhere, the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, knowingly and intentionally conspired and agreed with one another and with conspirators known and unknown to the Grand Jury to commit offenses against the United States, that is:

a. to intentionally access a computer without authorization and exceed authorized access, and thereby obtain information from any protected computer, for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i);

b. to knowingly and with intent to defraud access a protected computer without authorization and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Section 1030(a)(4); and

c. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to 10 or more protected computers during any one year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(A)(i)(VI).

Manner and Means of the Conspiracy

It was part of the conspiracy that:

7. The Defendants agreed, combined, and worked together with each other and others, known and unknown to the grand jury, to operate an online service called [redacted]

8. [redacted], a counter antivirus service, provides information that computer hackers can use to determine whether the computer viruses and other malware they create will be detected by antivirus software, including and especially antivirus software used by the computer systems of major United States retailers, financial institutions, government agencies, and other high-value targets. The purpose of [redacted], and the intent of the defendants in operating the service, is to allow computer hackers to develop malware, in particular, to make changes to their malware so as to reduce the chances that the malware will be detected by the antivirus applications and services of the companies and institutions they target.

9. [redacted] is one of the largest services of its kind and has at least 30,000 users. Malware that has been submitted to [redacted] includes some of the most prolific malware known to the Federal Bureau of Investigation (FBI) and has been used in major computer intrusions committed against American businesses.

10. The malware submitted to [redacted] includes, but is not limited to, the following:

a. **"Crypters"**: software used to hide malicious files from antivirus software so that the software cannot detect and quarantine the malicious files;

b. **"Remote Access Trojans"**: software that allows a remote "operator" to control a system as if he or she has physical access to that system, including the possibility of administrator-level privileges;

c. **"Keyloggers"**: surveillance software that has the capability to record keystrokes entered on the victim computer and send that information to the user of the keylogger. A keylogger can record and steal any information typed on a keyboard, including sensitive information such as emails, instant messages, and passwords to email, social media, and financial accounts; and

d. **"Malware Tool Kits"**: toolkits specifically designed for users to create customized malicious files with functions of user preference. Some of the toolkits have embedded [redacted] Application Program Interface (API) in order to determine if the created malicious files were detected by antivirus software. Typically, if the malicious files were detected by antivirus software, users would change the digital signature of the malicious files and rescan the malicious files using the [redacted] service with the goal of making the malicious files fully undetectable by antivirus software.

11. The Defendants intentionally marketed [redacted] to computer hackers using the website [redacted] and a hidden service accessible via The Onion Router (TOR), an online network for enabling anonymity. The Defendants also advertised [redacted] on underground online cybercrime forums, which are support networks used by individuals worldwide to buy, sell, and rent malware kits, botnets, and stolen personal identifying information (PII). Moreover, the [redacted] service differed from legitimate scanning services in multiple ways. For example, while legitimate scanning services share data about uploaded files with the antivirus community,

and notify their users that they will do so, [redacted] instead informed its users that they could upload anonymously, and that data about uploaded files would not be shared with the antivirus community. As a result, the Defendants knew and intended that the [redacted] service would be used for facilitation of online criminal activity.

12. The Defendants were leaders of the conspiracy and played the following roles, among others:

a. RUSLANS BONDARS served as an administrator of [redacted] BONDARS'S responsibilities in the conspiracy included, among other things, maintaining the technical infrastructure used for the [redacted] service and website;

b. JURIJS MARTIŠEVS also served as an administrator of [redacted] MARTIŠEVS'S responsibilities in the conspiracy included, among other things, providing customer support to [redacted] customers, typically via email, ICQ, Jabber, and Skype.

Overt Acts

In furtherance of the conspiracy and its objects, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere by members of the conspiracy:

13. On or about October 3, 2006, MARTIŠEVS registered for a PayPal account under the business name [redacted]

14. One of the Defendants' co-conspirators, Z.S., was a malware developer who operated, in part, from Great Falls, Virginia, within the Eastern District of Virginia. Z.S. designed a keylogger that he sold to over 3,000 customers, who in turn infected over 16,000 computers and thereby stole information, such as passwords, from those computers. On or about November

18, 2012, Z.S., using a computer in the Eastern District of Virginia, caused a payment to be made to an account controlled by the Defendants.

15. In exchange for this payment and others, the Defendants provided Z.S. with access to [redacted] and allowed Z.S. to integrate the [redacted] API tool directly into his keylogger toolkit. The integration of the [redacted] tool into Z.S's keylogger allowed Z.S.'s customers to scan the keylogger's executable file to determine if the executable file would be detected by antivirus companies. If the executable was detected, the user could change the file's digital signature and rescan the executable, with the goal of making the malware fully undetectable by antivirus software.

16. On or about November 18, 2012 through on or about November 23, 2012, Z.S., using a computer located in the Eastern District of Virginia, and MARTIŠEVS exchanged emails regarding Z.S.'s access to the [redacted] service.

17. Beginning at least on or around October 28, 2009, and continuing through the present, MARTIŠEVS communicated with customers and potential customers of [redacted] via ICQ, an instant messaging system, in order to provide customer support and discuss the benefits and terms of [redacted] membership. At all relevant times, ICQ employed servers within the Eastern District of Virginia. Accordingly, MARTIŠEVS'S ICQ messages, which were sent in furtherance of the conspiracy, involved a wire signal being sent into, and typically out of, the Eastern District of Virginia.

18. On or about February 1, 2013, through on or about July 15, 2014, BONDARS accessed the [redacted] service and site and performed administrative functions in furtherance of the conspiracy while logged into cloud storage space that was controlled by the conspiracy and hosted on servers owned by Amazon Web Services within the Eastern District of Virginia. In

order to access the [redacted] service and site from outside the United States through the Amazon cloud storage, BONDARS caused wire signals to be transmitted both into and out of the Eastern District of Virginia.

(All in violation of Title 18, United States Code, Section 371.)

COUNT 2

18 U.S.C. § 1349
(Conspiracy to Commit Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

19. The factual allegations contained in paragraphs 1 through 18 are realleged and incorporated by reference herein.

20. From at least on or about October 3, 2006, and continuing until at least the date of this Indictment, in the Eastern District of Virginia and elsewhere, the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, knowingly and intentionally conspired and agreed with one another and with conspirators known and unknown to the Grand Jury to commit Wire Fraud, in violation of 18 U.S.C. § 1343, that is, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, to transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice.

21. At all relevant times, the Defendants acted with the intent to defraud.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

22. As specified in more detail above, the Defendants agreed, combined, and worked together with each other and others, known and unknown to the grand jury, to operate an online service called [redacted]

23. The Defendants' chief purpose in operating the [redacted] service was to enable and cause fraud to be committed by and through co-conspirators who were [redacted] members

and by their co-conspirators, accomplices, and agents. The Defendants knew that their customers were using [redacted] for the purpose of furthering fraudulent schemes that were furthered by interstate and foreign wire signals and acted with the purposes of furthering these fraudulent schemes. Specifically, the Defendant's chief purpose in operating the [redacted] service was to help develop malware that could be used to gain unauthorized access to computer systems through false representations and thereby steal information, including sensitive financial and personal identifying information that could then be used to commit fraud.

Overt Acts

24. The overt acts specified in paragraphs 13 through 18 above were also committed in furtherance of the Wire Fraud conspiracy alleged in the instant count.

25. In addition, malware that was developed by the defendants' co-conspirators, who were [redacted] members located in the Eastern District of Virginia and elsewhere, with the assistance of MARTIŠEVS, BONDARS, and the [redacted] service, were used to perpetrate computer intrusions within the Eastern District of Virginia and elsewhere. The purpose of these computer intrusions was to steal information, including financial and personal identifying information, that could be used to commit fraud, and transfer that information via the internet across state and national lines to servers controlled by members of the conspiracy and their accomplices.

(All in violation of Title 18, United States Code, Section 1349.)

COUNT 3

18 U.S.C. §§ 1343 and 2
(Wire Fraud and Aiding and Abetting)

THE GRAND JURY FURTHER CHARGES THAT:

26. The factual allegations contained in paragraphs 1 through 25 are realleged and incorporated by reference herein.

27. From at least on or about October 3, 2006, and continuing until at least the date of this Indictment, in the Eastern District of Virginia and elsewhere, the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343. At all relevant times, the Defendants acted with the intent to defraud.

28. In particular, as specified above, the Defendants operated the [redacted] service for the purpose of gaining access to computers through false representations and through that access stealing information, including but not limited to financial and personal identifying information such as credit card, social security numbers, and dates of birth, and for the purpose of using that fraudulently obtained information for, among other purposes, making fraudulent purchases and fraudulent withdrawals and transfers of funds.

29. In addition to committing Wire Fraud themselves, the Defendants also knowingly and intentionally aided and abetted Wire Fraud committed by [redacted] customers and their accomplices. At all times, the Defendants knew that their customers were using their service for

the purpose of furthering fraudulent schemes that were furthered by wire signals and committed the acts specified in this indictment for the purposes of furthering the fraudulent schemes of their customers and their accomplices and co-schemers and with the intention of causing them to be committed.

30. Specifically, as specified in paragraph 25, the Defendants provided the [redacted] service to accomplices and co-schemers in the Eastern District of Virginia and elsewhere, knowing that it would be used to develop malware to access computer systems by means of false representations and thereby steal information from those computer systems located in the Eastern District of Virginia and elsewhere, including sensitive financial information, and for the purpose of using the stolen information to commit fraud. The Defendants at all times knew that the [redacted] service was being used to further such fraudulent schemes and acted for the purpose of furthering these crimes and causing them to be committed.

(All in violation of Title 18, United States Code, Sections 1343 and 2.)

COUNT 4

18 U.S.C. §§ 1030(a)(5)(A) and 2
(Computer Intrusion with Intent to Cause Damage and Aiding and Abetting)

31. The factual allegations contained in paragraph 1 through 30 are realleged and incorporated by reference herein.

32. On or about October 15, 2012 through on or about December 2014, within the Eastern District of Virginia and elsewhere, the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, knowingly and intentionally aided and abetted computer intrusions with the intent to cause damage, in violation of 18 U.S.C. § 1030(a)(5)(A).

33. In particular, the Defendants sold their [redacted] service to Z.S., a malware developer located in the Eastern District of Virginia, knowing that Z.S. intended to use [redacted] to develop malware which would be used to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization to 10 or more protected computers during any one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(A)(i)(VI).

34. On or about November 18, 2012, with this knowledge, and with the intent and purpose of aiding such unlawful computer intrusions and causing them to be committed, the Defendants provided Z.S. with access to the [redacted] service.

35. Z.S. then used [redacted] to help shield his malware from detection by antivirus software and to offer his customers the ability to use the [redacted] service themselves to help avoid detection from the antivirus software of the victim computers they targeted. With the aid of the [redacted] service provided by the Defendants, Z.S. sold his malware to over 3,000 customers who in turn accessed over 16,000 computers without authorization and thereby intentionally damaged those computers by changing their functioning such that those computers recorded

sensitive information such as account passwords and sent that information to the users of Z.S.'s keylogger without the authorization of the owners of the victim computers.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 2.)

NOTICE OF FORFEITURE

18 U.S.C. §§ 981, 2323; and 28 U.S.C. § 2461

THE GRAND JURY HEREBY FINDS THAT:

36. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

37. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, that in the event of their conviction of any of the offenses charged in this Indictment, the United States intends to forfeit the Defendants' property as further described in this NOTICE OF FORFEITURE.

38. Upon conviction of any of the accounts alleged in the indictment, the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the violation, pursuant to 18 U.S.C. § 981(a)(1)(C) and (D)(vi), and 28 U.S.C. § 2461(c).

MONEY JUDGMENT

39. The United States of America gives notice to the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, that upon conviction, a money judgment may be imposed equal to the total value of the property subject to forfeiture, which is at least $125,769.87.

PROPERTY SUBJECT TO FORFEITURE

40. The United States of America gives notice to the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS, that the property to be forfeited includes, but is not limited to:

a. PayPal account under the name [redacted] with account number ending in 5280;

b. Liberty Reserve account under the name "Jurijs," with account number ending in 0140;

c. WebMoney account under the name Jurijs Martisevs, with identification number ending in 8563;

d. Swedbank account, with Swift Code HABALV22, and account number ending in 0608.

SUBSTITUTE ASSETS

41. If any of the property described above, as a result of any act or omission of the Defendants, RUSLANS BONDARS and JURIJS MARTIŠEVS,

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to and intends to seek forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 2323(b)(2)(A) and 28 U.S.C. § 2461(c).

(All pursuant to 18 U.S.C. §§ 981, 2323; and 28 U.S.C. § 2461.)

A TRUE BILL:

* Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: Kellen Dwyer
Kellen S. Dwyer
Assistant U.S. Attorney

Ryan K. Dickey
Senior Counsel, Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division